Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 6 (4): 342-355, 2014
ISSN 1815-7432 / DOI: 10.3923/rjit.2014.342.355

Encrypted Secret Blend with Image Steganography for Enhanced Imperceptibility and Capacity

M. Padmaa and Y. Venkataramani
Saranathan College of Engineering, Trichirapalli, Tamilnadu, India

Corresponding Author: M. Padmaa, Saranathan College of Engineering, Trichirapalli, Tamilnadu, India

ABSTRACT

This study deals with a novel steganographic technique which demonstrates dynamic encryption based image steganographic technique in the spatial domain that hides message inside another carrier color image where the authenticated receiver can only extract this embedded secrete using the secrete key(s). This study proposed to merge the imperceptibility of pixel indicator embedding technique along with multiple key encryptions. The trap lies in encrypting the raw data into four sets of messages D1, D2, D3 and D4, say using four different keys K1, K2, K3 and K4, respectively. The encrypted messages are then embedded into cover image producing 4 stego objects. From these object, deviations of each row with respect to the cover are compared and based on minimum error, the corresponding row is selected to form the final image, thereby constructing a final image superior to its parent images. This technique also provides with suitable security owing to the fact that the concealed data cannot be deciphered until the appropriate parent key is used for the appropriate row.

Key words: Cryptography, data hiding, information security, steganography, pixel indicator

INTRODUCTION

Man has trampled in an era where almost everything and everyone is hooked to the internet. With advent of path breaking technologies, these sophisticated gadgets have significantly reduced in dimension leading this espionage to calamitous level. A majority of these inventions contribute solely to the field of communication, making the world smaller for the technically equipped humans. This has been the driving force towards collection and assimilation of huge chunks of data round the globe. However, this also led to the need for various security measures that need to be taken to protect the identity and the nature of information from adversaries while allowing our comrades to access them. This paved the way towards the birth of cryptography where the concerned data was rendered itself as incomprehensible unless the seeker had the key to modify and understand the message. But with the exponentially increasing computational capabilities, one needed to find a more discreet and covert modes of communication. Information hiding was able to answer to this requirement (Amirtharajan and Rayappan, 2012a-d, 2013; Amirtharajan *et al*., 2010, 2011, 2013a-j; Cheddad *et al*., 2010; Janakiraman *et al*., 2012a, b, 2014a, b; Luo *et al*., 2011; Mohammad *et al*., 2011; Salem *et al*., 2011; Ramalingam *et al*., 2014a, b; Thien and Lin, 2003; Zhao and Luo, 2012).

The present day world has been revolving around the rising communication technology and its various effects. The need of the hour can be critically stated as the security of the millions of data transmitted over the communication channel. While there have been very good techniques developed every day there are many people who increasingly get access to the secured data in an unauthorized manner (Amirtharajan and Rayappan, 2012a-d, 2013; Cheddad *et al*., 2010;

Chan and Cheng, 2004). Internet has been elevated as one of the highly used communication means in the recent times. It is the easiest means to transmit data around the world. Cryptography along with steganography has turned up in front of us, as a lethal weapon or face saving technique to preserve the valuable information from the eavesdroppers reach (Padmaa *et al*., 2011; Padmaa and Venkataramani, 2014a, b; Rajagopalan *et al*., 2012a, b, 2014a-d).

Cryptography is the art of encrypting data which can be achieved by versatile algorithms. Steganography refers to concealing the existence of data itself by means of combining it with other forms of data like images (Wu and Tsai, 2003; Janakiraman *et al*., 2012a, b, 2013; Amirtharajan and Rayappan, 2012b; Thanikaiselvan *et al*., 2012a-c, 2013a, b), audios and videos etc. Combination of the two methods can materialize into a methodology which has the qualities inherited from both. The main motto of this study is to increase the imperceptibility when an image is used as a means for hiding data. Imperceptible means to be as subtle as possible or to be unidentifiable.

Information hiding is a communication game between an information hider and an attacker, in which information is available only to the information hider and to the decoder. Characteristics expected from information hiding vary for every type of application depending on some of the prime features such as imperceptible, robustness, security etc. andsecure communication is recent through OFDM and Spread Spectrum is vital for information security (Thenmozhi *et al*., 2012; Praveenkumar *et al*., 2012a, b, 2013a, b, 2014a-j).

The simple classification on steganography is spatial or transform (Amirtharajan and Rayappan, 2013), further classified based on cover like text, image, video and audio (Cheddad *et al*., 2010; Amirtharajan *et al*., 2012; Amirtharajan and Rayappan, 2013). After knowing the existing method this study focused on Image steganography.

METHODOLOGY

Present study, uses four keys to encrypt the secret data and embed in the same cover image, thus producing 4 different stego images respectively, virtually imperceptible to the human eye but prone to stego analysis and its statistical attacks. Hence, to avoid this, by distributed error in all the 3 planes taking advantage of the presence of the different channels available in a color image. Instead of embedding in a single plane, in this proposed method used Pixel Indicator technique to distribute error in all three planes based on Pixel Indicator.

To increase the security level, pseudo random sequence generator is used to select the order of the rows initially and then an indicator plane/channel governs the embedding of data between the other two channels (data channels). In the color image, the red plane can be chosen as the indicator plane wherein the least significant bits in every pixel in this channel is used to decide the embedding. Throughout this embedding process, the indicator plane/channel is not to be altered since then this method cannot recover the data if it is modified/tampered/edited etc.

Since, the data to be hidden is usually embedded in predetermined fashion of k bits. Present method used Optimal Pixel Adjustment Process to further reduce the mean square error. Once the above mentioned processes are completed and 4 stego images are generated every row from these are compared against the corresponding row in cover image. This step allows determining the relative deviation of each of these with respect to the cover image.

The stego object which provides the least deviation for the concerned row contributes to the formation of the particular row in the new hybrid stego image, thereby acting as the parent image for it. Thus, the hybrid image is a composition of rows from 4 different parents providing suitably lower error rates. This also produces a certain cryptic effect as the user would need to know the genetic sequence in which the rows were formed. This acts as another key which can be passed to the authorized user alone to prevent malicious users from deciphering the data (Fig. 1).

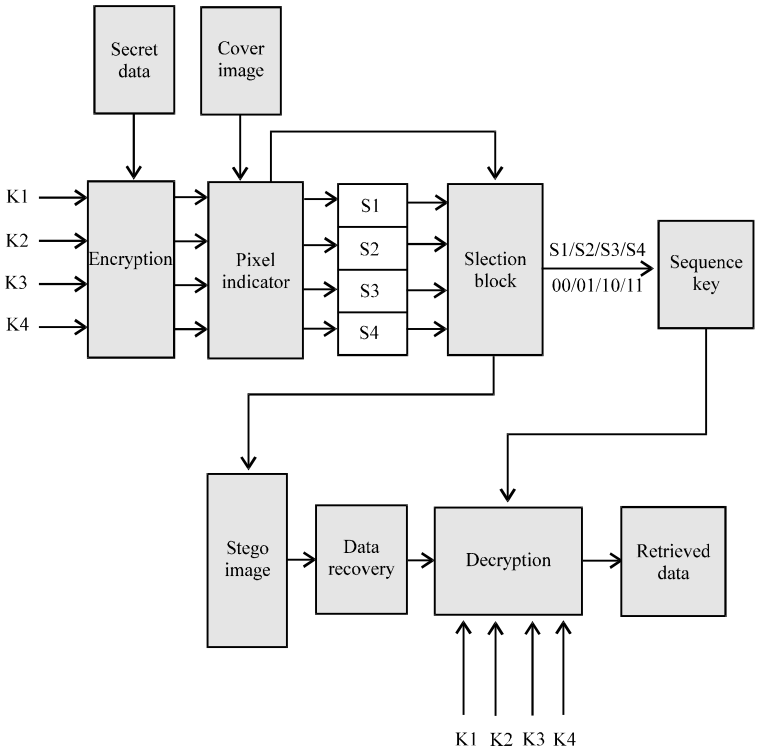

Fig. 1: Proposed block diagram

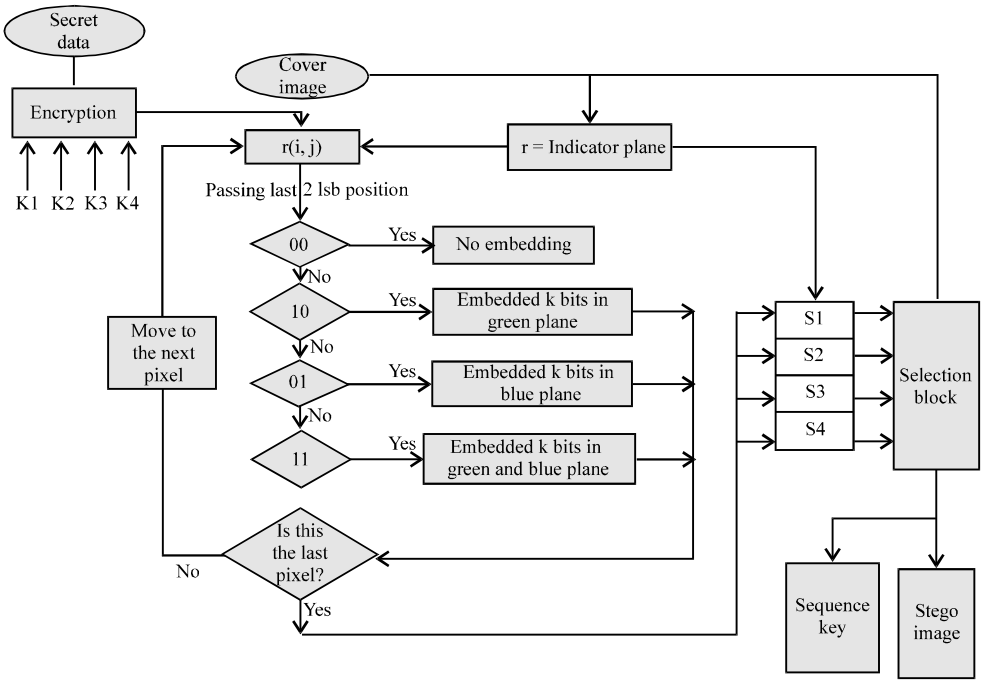

Fig. 2: Proposed flowchart for embedding

The proposed flowchart for embedding secret shows in Fig. 2.

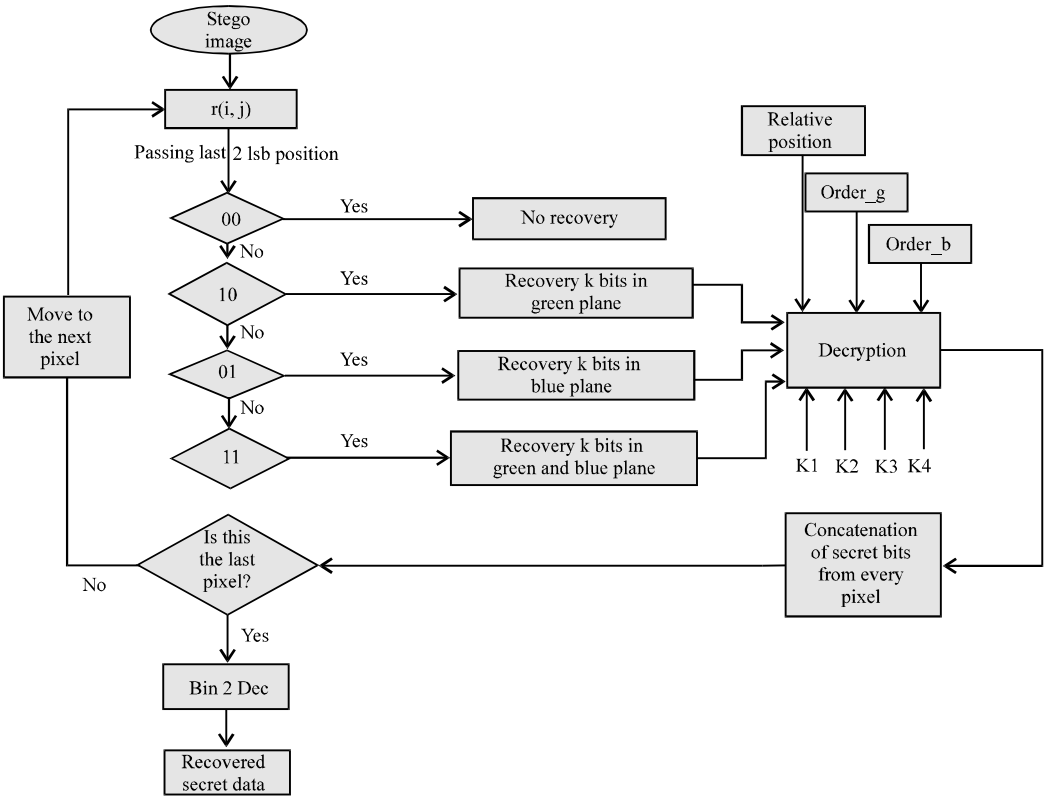

Fig. 3: Flowchart for extraction

The proposed flowchart for extracting the secret is shown in Fig. 3.

Embedding algorithm:

Inputs: Cover image, four 8-bit user defined secret keys, message, Number of bits to embed (k)

Intermediate outputs: The 4 parent stego images each formed using its individual key

Outputs: Stego image, order sequences

Step 1: Encrypt the secret data using the four user defined keys (key1, key2, key3, key4) and Store them in 4 different variables - (datk1, datk2, datk3, datk4)

Step 2: Convert the encrypted data sequence into binary sequence and store them in (dat_k1, dat_k2, dat_k3, dat_k4)

Step 3: Pseudo random sequence generator is enabled to select the order of the rows in which the data to be hidden

Step 4: Isolate the Red(R), Green (G) andBlue (B) components of the cover image

Step 5: Check each pixel of R for the following condition:

Consider the 2 LSB positions for the pixel in ith row and jth column in R (indicator)plane:

If r(i, j,7) = 0 and r(i, j, 8) = 0 then no embedding

else If r(i, j, 7) = 0 and r(i, j, 8) =1 then embed k bits in green plane in the respective i, j pixel

else If r(i, j, 7) = 1 and r(i, j, 8) = 0 then embed k bits in blue plane in the respective i,j pixel

else embed k bits in green and then blue planes in the respective i,j pixel

Step 6: Repeat step 4 till all the bits from the secret data have been embedded

Step 7: Store the Red(R), stego-green (G) and stego-blue (B) planes in a new color stego image (steg1 etc.,)

Step 8: Perform step 4 and 5 using all the 4 binary data sequences to obtain 4 different stego images (steg1, steg2, steg3, steg4)

Step 9: Compare the 4 stego images with the original cover row wise to obtain their deviations respectively (for each plane)

Step 10: Select the rows with minimum deviation, from each of the planes to form a new final Stego-image with the selected plane consisting of a combination which results from all the 4 parent stego images

Step 11: Simultaneously while selecting the row generate an order sequence which defines:

Row taken from steg1-00
Row taken from steg2-01
Row taken from steg3-10
Row taken from steg4-11

This will result in a order sequence per plane of 2×(number of rows in the cover image)

Step 12: Store the order sequences as order_p1…… etc., respective to the planes

Step 13: The Final stego-image and the 2 order sequences are to be transmitted suitably

Extracting algorithm:

Input: Stego image, Order sequences, four 8-bit keys, Number of bits embedded (k)

Output: Recovered data

Step 1: Read ith, jth pixel of r (indicator plane) and then:

Consider the 2 LSB position
if r(i, j,7) = 0 and r(i, j, 8) = 0 then perform no action
if r(i, j, 7) = 0 and r(i, j, 8) =1 then read and store k bits from green plane in the concerned pixel. These k bits can be decrypted by knowing the relative position and the order of the ith row in the green plane
if r(i, j, 7) =1 and r(i, j, 8) = 0 then read and store k bits from blue plane in the concerned pixel
These k bits can be decrypted by knowing the relative position and the order of the ith row in the blue plane
If r(i, j, 7) =1 and r(i, j, 8) =1 then read and store k bits from both green and blue planes respectively in the concerned pixel. These 2k bits can be decrypted by the relative knowledge of the position and the order of the ith row in the green plane and blue plane (relative position is the modulo-8 value of the count of number of bits being read and stored)

Step 2: Concatenate the k bits as a binary decrypted sequence and perform step 1 with the next pixel position until the end of the image or till we have received the entire data embedded

Step 3: Convert the binary sequence into its original form (decimal/character) to see the final recovered data

RESULT AND DISCUSSION

Three color cover images of Temple, Lena and Baboon of dimension 256×256 are taken to verify the performance of this algorithm. These images go through the testing of full embedding capability. To have a vision about the efficacy, corresponding stego images are generated and studied Fig. 4-6. The Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) can be used to determine how the original cover image has been affected by the embedded message. Though the MSE and PSNR show that there has been degradation in the in the original image, these degradations are visually imperceptible. The MSE and PSNR values are calculated, tabled and compared (Table 1).

The other important parameter is the SSIM index which is almost close to unity which implies that there is no much deviation between the original image and the stego image generated. The security of the embedded message is very good because here we used 4 individual 8-bit user defined

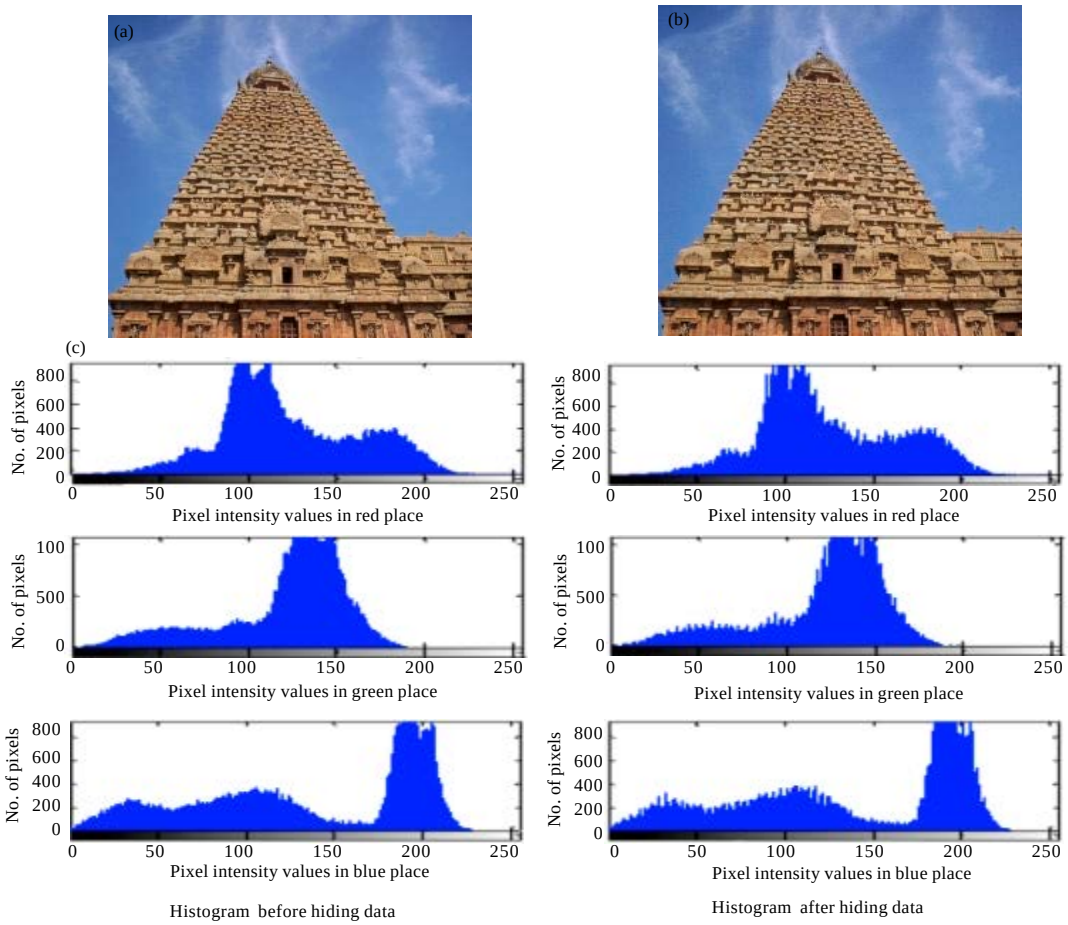

Fig. 4(a-c): Color cover image of Temple (a) Cover image, (b) Stego image and (c) RGB histogram of stego image

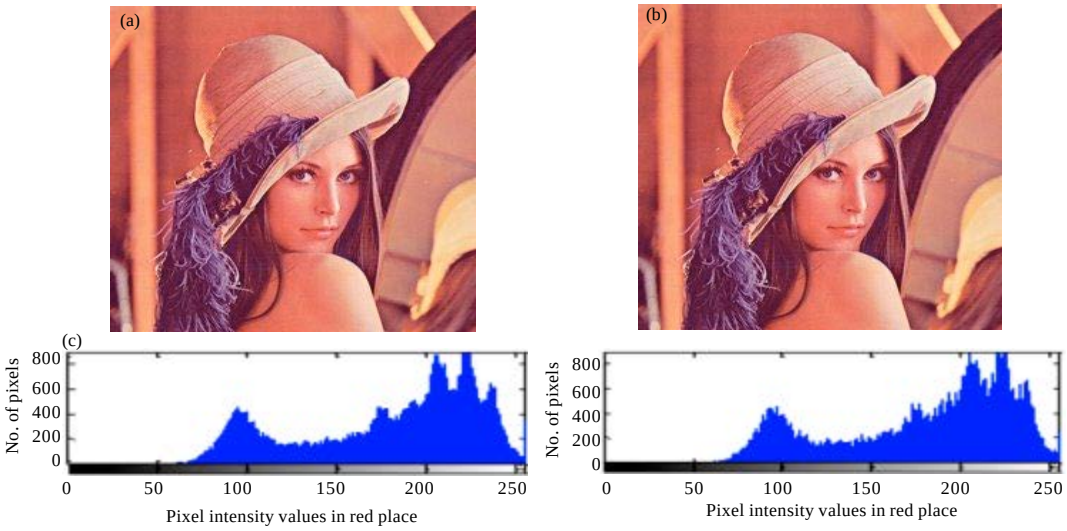

Fig. 5(a-c): Continue

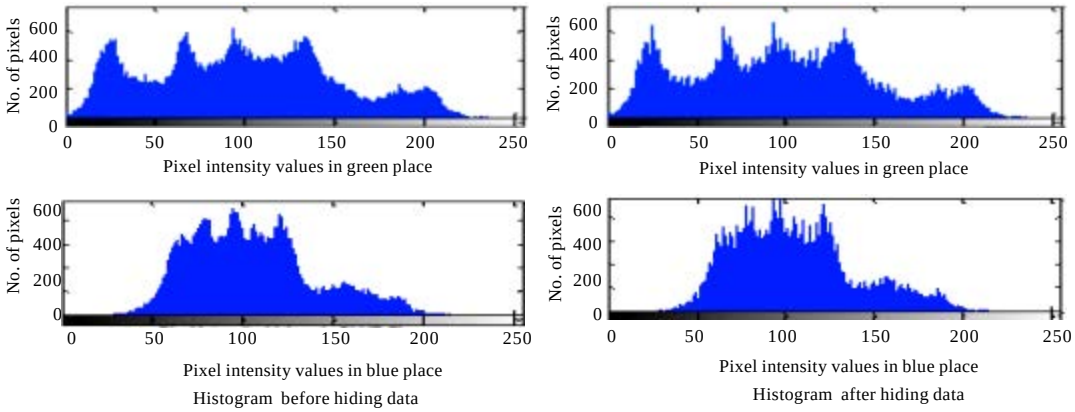

Fig. 5(a-c): Color cover image of Lena (a) Cover image, (b) Stego image and (c) RGB histogram of stego image

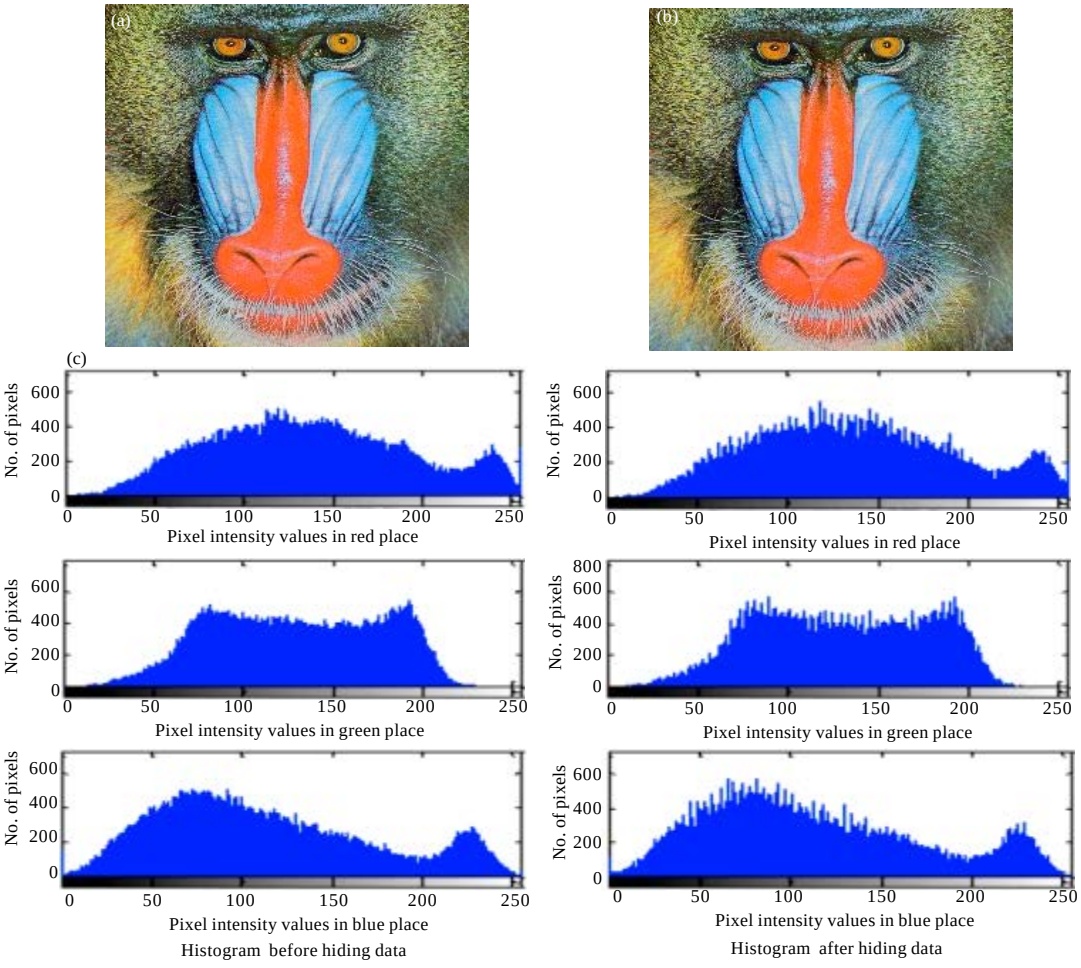

Fig. 6(a-c): Color cover image of Baboon (a) Cover image, (b) Stego image and (c) RGB histogram of stego image

Table 1: MSE and PSNR values for intermediate stego images (Red plane as indicator)

		Red plane		Green plane		Blue plane	
Image	No. of bits embedded per pixel (k)	MSE	PSNR	MSE	PSNR	MSE	PSNR
Temple	1	0	∞	0.0756	59.3431	0.0741	59.4343
	2	0	∞	0.3558	52.6186	0.3458	52.7423
	3	0	∞	1.5703	46.1709	1.5468	46.2365
	4	0	∞	5.5167	40.7140	5.5708	40.6716
Lena	1	0	∞	0.0754	59.3598	0.0759	59.3265
	2	0	∞	0.3549	52.6294	0.3564	52.6114
	3	0	∞	1.5529	46.2193	1.5904	46.1158
	4	0	∞	5.4797	40.7433	5.6830	40.5850
Baboon	1	0	∞	0.0756	59.3431	0.0750	59.3827
	2	0	∞	0.3583	52.5887	0.3551	52.6268
	3	0	∞	1.5630	46.1911	1.5510	46.2248
	4	0	∞	5.4908	40.7344	5.4922	40.7334

keys which are required to recover the message. But even if the keys are known without knowing the order sequence of each plane it becomes very hard to recover the original data. Order sequence is the row-key mapping to decrypt the retrieved data from the embedded stego image.

Peak Signal to Noise Ratio (PSNR): The PSNR is calculated as follows:

$$PSNR = 10\log_{10}\left(\frac{I^2 max}{MSE}\right)dB \tag{1}$$

where, i_{max} is the maximum pixel value of image.

Mean Square Error (MSE): The MSE is calculated by using the following equation:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(C_{i,j} - S_{i,j}\right)^2 \tag{2}$$

where, M and N represent the total number of pixels in the horizontal and the vertical dimensions of the image $C_{i,j}$ represents the pixels in the original image and Si, j, represents the pixels of the stego-image.

Mean Structural SIMilarity Index (MSSIM): Mean SSIM (MSSIM) index is used to evaluate the overall image quality by using the following equation:

$$MSSIM(X, Y) = \frac{1}{M}\sum_{j=1}^{M} SSIM\left(X_j, Y_j\right) \tag{3}$$

$$MSSIM(X, Y) = \frac{\left(2\mu_x\mu_y + C_1\right)\left(2\sigma_{xy} + C_2\right)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)}$$

The value of MSSIM is in the interval [1, 0]. The value 1 means that the two images are exactly the same and 0 means totally unrelated. Bit error rate (BER) computes the actual number of bit positions which are changed in the stego-image compared with cover image:

Embedding capacity = Bits ebedded per pixel×No. of pixels in thje cover image

From Table 2, It's noted that Temple offer better imperceptibility without compromising capacity and MSSIM is also close to 1 for k = 1, 2 and 3 but for K = 4 its value 0.925. So k = 1, 2 till 3 and this proposed method is good.

From Table 3, It's noted that Lena offer better Imperceptibility without compromising Capacity and MSSIM is also close to 1 for k = 1,2 and 3 but for K = 4 its value 0.9437. So k = 1,2 till 3. This proposed From Table 4 It's noted that Baboon offer better Imperceptibility without compromising Capacity and MSSIM is also close to 1 for k = 1, 2 and 3 but for K = 4 its value 0.9860. So k = 1, 2 till 3.

From Table 5, It's noted that Baboon offer better imperceptibility without compromising capacity. In comparison with available result this method offers better capacity with less PSNR.

Table 2: Temple stego images with other metrics (Red plane as indicator)

Cover image of Temple	Plane	BER	MSE	PSNR	MSSIM	Total bits embedded
k = 1	Red	0	0	∞	1	65302
	Green	0.0284	0.2269	54.5719	0.9986	
	Blue	0.0278	0.2222	54.6631	0.9985	
k = 2	Red	0	0	∞	1	130604
	Green	0.0609	1.0674	47.8474	0.9934	
	Blue	0.0594	1.0375	47.9711	0.9934	
k = 3	Red	0	0	∞	1	195906
	Green	0.0918	4.7110	41.3997	0.9729	
	Blue	0.0903	4.6404	41.4653	0.9722	
k = 4	Red	0	0	∞	1	261208
	Green	0.1236	16.5501	35.9428	0.9245	
	Blue	0.1220	16.7124	35.9004	0.9199	

Table 3: Lena stego images with other metrics (Red plane as indicator)

No. of bits embedded per pixel (K bits)	Plane	BER	MSE	PSNR	MSSIM	Total bits embedded
4	Red	0	0	∞	1	261780
	Green	0.0819	10.9724	37.7278	0.9437	
	Blue	0.0830	11.3156	37.5940	0.9359	
3	Red	0	0	∞	0.9813	196335
	Green	0.0603	3.0388	43.3037	0.9823	
	Blue	0.0607	3.1012	43.2156	0.9800	
2	Red	0	0	∞	0.9956	130890
	Green	0.0393	0.6982	49.6913	0.9959	
	Blue	0.0396	0.7064	49.6404	0.9953	
1	Red	0	0	∞	0.9991	65445
	Green	0.0184	0.1470	56.4571	0.9991	
	Blue	0.0183	0.1467	56.4670	0.9990	

Table 4: Baboon stego images with other metrics (Red plane as indicator)

No. of bits embedded per pixel (K bits)	Plane	BER	MSE	PSNR	MSSIM	Total bits embedded
4	Red	0	0	∞	0.9829	261824
	Green	0.0822	10.8867	37.7619	0.9836	
	Blue	0.0818	10.8316	37.7839	0.9860	
3	Red	0	0	∞	0.9953	196368
	Green	0.0603	3.0323	43.3130	0.9953	
	Blue	0.0601	3.0375	43.3056	0.9960	
2	Red	0	0	∞	0.9989	130912
	Green	0.0399	0.7149	49.5881	0.9989	
	Blue	0.0397	0.6935	49.7204	0.9991	
1	Red	0	0	∞	0.9998	65456
	Green	0.0181	0.1448	56.5234	0.9998	
	Blue	0.0181	0.1448	56.5239	0.9998	

Table 5: Proposed method performance with comparative results

	Channel red		Channel green		Channel blue			
PI methods	MSE	PSNR	MSE	PSNR	MSE	PSNR	Bits per pixel	No. of bits embeded
Lena								
Proposed	3.862	42.26	3.6575	42.499	3.7719	42.3652	3.9944	261780
Amirtharajan *et al*. (2013b)	0.4987	51.15	0.2594	53.9904	0.7033	49.6593	1.9958	130798
Padmaa *et al*. (2011)	1.227	47.24	1.3641	46.782	1.02	48.045	2.114	138549
Amirtharajan *et al*. (2010)	1.68	45.89	1.57	46.180	1.52	46.31	2.13	139592
Amirtharajan *et al*. (2011)	1.2906	47.02	1.2374	47.2059	1.2049	47.3213	2.3139	151645
Amirtharajan *et al*. (2012)	2.4387	44.26	2.3066	44.501	2.3389	44.441	3.9181	256776
Baboon								
Proposed	3.7111	42.44	3.6289	42.5331	3.6105	42.5551	3.9951	261824
Amirtharajan *et al*. (2013b)	0.4754	51.35	0.2587	54.0024	4.6733	41.4345	1.9858	130144
Padmaa *et al*. (2011)	4.065	42.04	4.002	42.108	4.2847	41.812	3.657	239262
Amirtharajan *et al*. (2010)	2.61	43.96	2.65	43.88	2.72	43.77	2.51	164496
Amirtharajan *et al*. (2011)	1.554	46.21	1.5544	46.2151	1.5904	46.1157	2.3975	157121
Amirtharajan *et al*. (2012)	2.3702	44.39	2.3255	44.4657	2.3619	44.3981	3.9232	257108
Temple								
Proposed	2.2806	44.55	2.2622	44.5855	2.2988	44.5158	3.9857	261208
Amirtharajan *et al*. (2013b)	0.4673	51.43	0.2569	54.0333	0.8289	48.9458	1.9921	130556
Padmaa *et al*. (2011)	1.853	45.45	1.766	45.662	1.632	46.003	2.352	154409
Amirtharajan *et al*. (2010)	1.85	45.45	1.76	45.66	1.63	46	2.3	150732
Amirtharajan *et al*. (2011)	1.1159	47.65	1.1062	47.6924	1.124	47.6232	2.4659	161604
Amirtharajan *et al*. (2012)	2.3143	44.49	2.3095	44.4957	2.3764	44.3716	3.924	257160

Application of Optimal Pixel Adjustment Process (OPAP) improves image quality and the results suggest that there is a good improvement in the SSIM index which indicates that the stego output is very close to the cover image.

CONCLUSION

By combining multiple key data encryption with pixel indicator, proposed method obtained very high imperceptibility with high capacity. Even if the keys are known, without knowing the order sequence of each plane it becomes very hard to recover the original data. Order sequence is the

row-key mapping to decrypt the retrieved data from the embedded stego image. The complexity of the proposed system is $(2^{32})\times(2^{512})$ i.e., 4 keys each of 8 bit is used and 2 bits are used to specify the order and the size of image is 256×256. Further enhancement along with this method compression and more encryption will offer more capacity and better security.

REFERENCES

Amirtharajan, R., D. Adharsh, V. Vignesh and R.J.B. Balaguru, 2010. PVD blend with pixel indicator-OPAP composite for high fidelity steganography. Int. J. Comput. Applic., 7: 31-37.

Amirtharajan, R., R.R. Subrahmanyam, P.J.S. Prabhakar, R. Kavitha and J.B.B. Rayappan, 2011. MSB over hides LSB: A dark communication with integrity. Proceedings of the IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application, December 12-14, 2011, Bangalore, Karnataka, India, pp: 1-6.

Amirtharajan, R., J. Qin and J.B.B. Rayappan, 2012. Random image steganography and steganalysis: Present status and future directions. Inform. Technol. J., 11: 566-576.

Amirtharajan, R. and J.B.B. Rayappan, 2012a. Brownian motion of binary and gray-binary and gray bits in image for stego. J. Applied Sci., 12: 428-439.

Amirtharajan, R. and J.B.B. Rayappan, 2012b. An intelligent chaotic embedding approach to enhance stego-image quality. Inform. Sci., 193: 115-124.

Amirtharajan, R. and J.B.B. Rayappan, 2012c. Inverted pattern in inverted time domain for icon steganography. Inform. Technol. J., 11: 587-595.

Amirtharajan, R. and J.B.B. Rayappan, 2012d. Pixel authorized by pixel to trace with SFC on image to sabotage data mugger: A comparative study on PI stego. Res. J. Inform. Technol., 4: 124-139.

Amirtharajan, R. and J.B.B. Rayappan, 2013. Steganography-time to time: A review. Res. J. Inform. Technol., 5: 53-66.

Amirtharajan, R., K. Karthikeyan, M. Malleswaran and J.B.B. Rayappan, 2013a. Kubera kolam: A way for random image steganography. Res. J. Inform. Technol., 5: 304-316.

Amirtharajan, R., M.V. Abhiram, G. Revathi, J.B. Reddy, V. Thanikaiselvan and J.B.B. Rayappan, 2013b. Rubik's cube: A way for random image steganography. Res. J. Inform. Technol., 5: 329-340.

Amirtharajan, R., P. Archana and J.B.B. Rayappan, 2013c. Why image encryption for better steganography. Res. J. Inform. Technol., 5: 341-351.

Amirtharajan, R., S. Sulthana and J.B.B. Rayappan, 2013d. Seeing and believing is a threat: A visual cryptography schemes. Res. J. Inform. Technol., 5: 435-441.

Amirtharajan, R., K.M. Ashfaaq, A.K. Infant and J.B.B. Rayappan, 2013e. High performance pixel indicator for colour image steganography. Res. J. Inform. Technol., 5: 277-290.

Amirtharajan, R., R. Subrahmanyam, J.N. Teja, K.M. Reddy and J.B.B. Rayappan, 2013f. Pixel indicated triple layer: A way for random image steganography. Res. J. Inform. Technol., 5: 87-99.

Amirtharajan, R., S.D. Roy, N. Nesakumar, M. Chandrasekar, R. Sridevi and J.B.B. Rayappan, 2013g. Mind game for cover steganography: A refuge. Res. J. Inform. Technol., 5: 137-148.

Amirtharajan, R., V. Rajesh, P. Archana and J.B.B. Rayappan, 2013h. Pixel indicates, standard deviates: A way for random image steganography. Res. J. Inform. Technol., 5: 383-392.

Amirtharajan, R., P.S. Priya and J.B.B. Rayappan, 2013i. Pixel indicated user indicator: A muxed stego. Res. J. Inform. Technol., 5: 73-86.

Amirtharajan, R., G. Devipriya, V. Thanikaiselvan and J.B.B. Rayappan, 2013j. High capacity triple plane embedding: A colour stego. Res. J. Inform. Technol., 5: 373-382.

Chan, C.K. and L.M. Cheng, 2004. Hiding data in images by simple LSB substitution. Pattern Recognit., 37: 469-474.

Cheddad, A., J. Condell, K. Curran and P. Mc Kevitt, 2010. Digital image steganography: Survey and analysis of current methods. Signal Process., 90: 727-752.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Pixel forefinger for gray in color: A layer by layer stego. Inform. Technol. J., 11: 9-19.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Firmware for data security: A review. Res. J. Inform. Technol., 4: 61-72.

Janakiraman, S., S. Rajagopalan, K. Thenmozhi, H.N. Upadhyay and J. Ramanathan *et al.*, 2013. Captivating CODEC Stego (CCS): A cover on camouflage. Res. J. Inform. Technol., 5: 160-170.

Janakiraman, S., J. Chakravarthy, B. Radhakrishnan, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014a. Cover as key and key as data: An inborn stego. Inform. Technol. J., 13: 1969-1976.

Janakiraman, S., K.V.S.K. Kumar, R.R.K. Reddy, A. Srinivasulu, R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014b. Humming bird with coloured wings: A feedback security approach. Inform. Technol. J., 13: 2022-2026.

Luo, H., Z. Zhao and Z.M. Lu, 2011. Joint secret sharing and data hiding for block truncation coding compressed image transmission. Inform. Technol. J., 10: 681-685.

Mohammad, N., X. Sun and H. Yang, 2011. An excellent Image data hiding algorithm based on BTC. Inform. Technol. J., 10: 1415-1420.

Padmaa, M., Y. Venkataramani and R. Amirtharajan, 2011. Stego on 2^n: 1 Platform for users and embedding. Inform. Technol. J., 10: 1896-1907.

Padmaa, M. and Y. Venkataramani, 2014a. Adaptive data hiding based on visual cryptography. J. Applied Sci., 14: 1674-1688.

Padmaa, M. and Y. Venkataramani, 2014b. Random image steganography using pixel indicator to enhance hiding capacity. J. Applied Sci., 14: 1798-1808.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Regulated OFDM-role of ECC and ANN: A review. J. Applied Sci., 12: 301-314.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Phase for face saving-a multicarrier stego. Procedia Eng., 30: 790-797.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2013a. Can we reduce PAPR? OFDM+PTS+SLM+STEGO: A novel approach. Asian J. Sci. Res., 6: 38-52.

Praveenkumar, P., M. Nagadinesh, P. Lakshmi, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013b. Convolution and viterbi EN(DE)coders on OFDM hides, rides and conveys message-A neural STEGO. Proceedings of the International Conference on Computer Communication and Informatics, January 4-6, 2013, Coimbatore, pp: 1-5.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014a. Sub carriers carry secret: An absolute stego approach. J. Applied Sci., 14: 1728-1735.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014b. Double layer encoded encrypted data on multicarrier channel. J. Applied Sci., 14: 1689-1700.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014c. Purposeful error on OFDM: A secret channel. Inform. Technol. J., 13: 1985-1991.

Praveenkumar, P., G.S. Hemalatha, B. Reddy, K. Thenmozhi, J.B.Bd. Rayappan and R. Amirtharajan, 2014d. Secret link through simulink: A stego on OFDM channel. Inform. Technol. J., 13: 1999-2004.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014e. Stego in multicarrier: A phase hidden communication. Inform. Technol. J., 13: 2011-2016.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014f. Inserted embedding in OFDM channel: A multicarrier stego. Inform. Technol. J., 13: 2017-2021.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014g. Data puncturing in OFDM channel: A multicarrier stego. Inform. Technol. J., 13: 2037-2041.

Praveenkumar, P., R. Deepak, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014h. Reversible steganography on OFDM channel: A role of cyclic codes. Inform. Technol. J., 13: 2047-2051.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014i. Reversible steganography on OFDM channel-a role of RS coding. Inform. Technol. J., 13: 2052-2056.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014j. Spread and hide-a stego transceiver. Inform. Technol. J., 13: 2061-2064.

Rajagopalan, S., R. Amirtharajan, H.N. Upadhyay and J.B.B. Rayappan, 2012a. Survey and analysis of hardware cryptographic and steganographic systems on FPGA. J. Applied Sci., 12: 201-210.

Rajagopalan, S., S. Janakiraman, H.N. Upadhyay and K. Thenmozhi, 2012b. Hide and seek in silicon: Performance analysis of Quad block Equisum Hardware Steganographic systems. Procedia Eng., 30: 806-813.

Rajagopalan, S., Y. Ravishankar, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014a. Modeling combo PR Generator for Stego Storage Self Test (SSST). Inform. Technol. J., 13: 1936-1944.

Rajagopalan, S., P.J.S. Prabhakar, M.S. Kumar, N.V.M. Nikhil, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014b. MSB based embedding with integrity: An adaptive RGB Stego on FPGA platform. Inform. Technol. J., 13: 1945-1952.

Rajagopalan, S., K. Pravallika, R. Radha, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014c. Stego on song-an amalgam of VI and FPGA for hardware info hide. Inform. Technol. J., 13: 1992-1998.

Rajagopalan, S., H.N. Upadhyay, S. Varadarajan, J.B.B. Rayappan and R. Amirtharajan, 2014d. Gyratory assisted info hide-a nibble differencing for message embedding. Inform. Technol. J., 13: 2005-2010.

Ramalingam, B., R. Amirtharajan and J.B.B. Rayappan, 2014a. LCC-LSB-FPGA stego-A reconfigurable security. J. Applied Sci., 14: 2139-2148.

Ramalingam, B., R. Amirtharajan and J.B.B. Rayappan, 2014b. Stego on FPGA: An IWT approach. Sci. World J. 10.1155/2014/192512

Salem, Y., M. Abomhara, O.O. Khalifa, A.A. Zaidan and B.B. Zaidan, 2011. A review on multimedia communications cryptography. Res. J. Inform. Technol., 3: 146-152.

Thanikaiselvan, V., P. Arulmozhivarman, J.B.B. Rayappan and R. Amirtharajan, 2012a. Graceful graph for graceful security-towards a STE (G) Raph. Res. J. Inform. Technol., 4: 220-227.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012b. Wavelet Pave the Trio travel for a secret mission: A stego vision. Global Trends Inf. Syst. Software Appl., 270: 212-221.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012c. Horse riding and hiding in image for data guarding. Procedia Eng., 30: 36-44.

Thanikaiselvan, V., P. Arulmozhivarman, S. Subashanthini and R. Amirtharajan, 2013a. A graph theory practice on transformed image: A random image steganography. Sci. World J. 10.1155/2013/464107

Thanikaiselvan, V., K. Santosh, D. Manikanta and R. Amirtharajan, 2013b. A new steganography algorithm against chi square attack. Res. J. Inform. Technol., 5: 363-372.

Thenmozhi, K., P. Praveenkumar, R. Amirtharajan, V. Prithiviraj, R. Varadarajan and J.B.B. Rayappan, 2012. OFDM+CDMA+Stego = Secure communication: A review. Res. J. Inform. Technol., 4: 31-46.

Thien, C.C. and J.C. Lin, 2003. A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern Recognit., 36: 2875-2881.

Wu, D.C. and W.H. Tsai, 2003. A steganographic method for images by pixel-value differencing. Pattern Recogn. Lett., 24: 1613-1626.

Zhao, Z. and H. Luo, 2012. Reversible data hiding based on Hilbert curve scan and histogram modification. Inform. Technol. J., 11: 209-216.